Mission Red Team Review Charter
For the
SORCE Mission
Approved 8/31/00

Mission Red Team Review Charter for
SORCE Mission

1. Background

In the light of some recent NASA mission failures and the resulting Failure Review Board findings, the NASA Administrator has requested that the Center Director conduct critical Red Team Reviews on each of the Center's missions prior to the mission launch. This review is to go beyond a review of the Project documentation of what was done and into technical aspects of the program and the remaining risk.

The implementation of these Reviews for the SORCE Mission will consist of two separate review processes conducted by separate teams. One process will cover the Mission aspects (i.e. Spacecraft and Mission Operations) and will be conducted by the Mission Red Team and the other will cover the launch vehicle aspects and will be conducted by the Launch Vehicle Services Red Team. KSC will establish the Launch Vehicle Services Red Team charter with concurrence by the GSFC and JPL Center Directors. Some cross-membership between the Mission Red Team and the Launch Vehicle Services Red Team shall be required in order to ensure that spacecraft and launch vehicle interfaces and related topics are properly reviewed. Cross-membership participants shall be selected by the Red Team Chairpersons (i.e. some members of the Mission Red team as selected by that team's chairperson will be on the Launch Vehicle Services Red Team for the Mission Unique Review (defined in the KSC Launch Vehicle Services Red team Charter) and vice versa.

Objective

The objective of this review will be to enhance the probability of the SORCE mission success by bringing to bear additional technical expertise to review all mission critical aspects of the program implementation.

2. Scope

The mission elements that will be addressed by the Red Team Review, and the depth to which each element will be addressed, shall be as follows:

- Spacecraft-fully addressed
- Payload-fully addressed
- Spacecraft launch preparations, launch event and launch support-fully addressed
- Spacecraft to launch vehicle integration-fully addressed
- Spacecraft required launch vehicle mission unique changes-fully addressed
- Readiness for on orbit operations-fully addressed
- Unique-to-mission changes to the ground station-fully addressed
- SOMO/institutional mission operations-addressed on a mission unique requirements basis only
- Mission science operations-limited to systems needed for data capture, processing, archiving and distribution only

3. Red Team Review Process

The Mission Red Team Reviews shall consist of a critical technical implementation and operations review on the mission implementation from the perspective of looking at what could go wrong and cause the mission to be less than fully successful. Specific key

processes used by the Project in the implementation of the mission shall be reviewed. The results of some of these key processes will be reviewed and assessed as well. From this information the Red Team shall identify and document all remaining risk that could be in-line with complete mission success.

The Red Team shall have a membership that is external to the GSFC and is independent of SORCE Project personnel. The Red Team will function as an overview team that can assign functions and work to specialized technical teams as appropriate. These specialized teams may be supported by the SORCE Project/ contractor personnel and will report in this capacity to the Red Team Chairperson. The core Mission Red Team is solely responsible for the implementation of these reviews and the Red Team Chairperson may request mission and contractor support as necessary.

Code 300 at the GSFC, acting for the GSFC Program Management Council (GPMC) shall be the coordinating and sponsoring organization for the Red Team.

The SORCE Project shall be required to assemble all pertinent information (using specific formats agreed to by the Red Team Chairperson) and present that information to the Red Team. It is expected that the standard two phases of the review will require about 2 to 3 days each (See Table 1). The Red Team final report will be presented at the time of the Mission Flight Readiness Review (MRR). The Red team shall have the authority to request that the Project prepare all necessary documentation and other records to enable and otherwise support these reviews. The Project shall also arrange for the cognizant peer review and systems review chairpersons to present the methodologies and findings of the individual reviews to the Red Team.

The Launch Vehicle Services Red Team Chairperson shall coordinate with the Mission Red team Chairperson when integrated presentations are necessary.

4. Review Process Specifics

The Project (or KSC for the launch related portions) shall prepare, assemble, and present data in specified formats, that addresses (or provides) the following:

1. The level, competence and independence of technical peer reviews that were performed on each of the elements and components (hardware and software)

2. The performance, level and independence of system level reviews that were conducted (hardware and software).

3. The level and thoroughness to which the test and verification program was implemented. The test and verification program at all levels from black box to spacecraft and integrated mission shall be detailed. This shall also include the validation and verification (V&V) and independent validation and verification (IV&V) processes used on software.

   Where IV&V has not been performed in compliance with draft NASA IV&V Policy and criteria (See Attachments B & C) assess the net value of performing IV&V at this stage in the program. Also identify any residual risks being taken in

the Project because of the lack of IV&V.

4. The level of mission assurance that was imposed on the implementation of the mission (hardware and software). This shall include parts usage as well as workmanship standards imposed. It shall also address the software assurance processes implemented.

5. The systems management imposed and implemented for the mission. This shall include the performance and thoroughness of analyses, requirement management, systems engineering, software metrics, configuration management, documentation and technical record keeping and workmanship and test process management.

6. Factors such as staffing and the experience of the implementing organization.

7. The results of the test and integration process of all of the hardware and software elements of the mission. This shall include information on the review and assessment of all failures and anomalies and their resolution.

8. Information on the failure-free as well as the total operating time on all mission critical hardware and software.

9. The results of the technical review process shall be detailed. It shall include an assessment of all RFA's and the Project responses to those RFA's.

10. The amount, level and fidelity of mission simulations and launch/operations training that was done or is planned to be done to prepare the mission for launch and on orbit operations including identification of all planned contingency operations and of those operations which were or will be practiced by the ops team. Identify any green card exercises (postulated mission contingencies which require action by the ops team) planned or conducted with the ops team. Provide a spacecraft mission timeline from liftoff to commencement of normal science operations and identify for each step the corrective action to be taken if the mission event does not occur as planned.

11. Provide the Failure Mode and Effects Analyses (FMEA) and the Fault Tree Analyses (FTA) that were performed for the program with appropriate annotations and tutorials. Provide the results of the Probability Risk Assessments (PRA) that were performed.

    Where these analyses have not been performed or are not complete, the Team shall assess the work that has been done and shall assess the situation in regards to available data for doing a FMEA, FTA, and a PRA that would include all non-core ELV elements of this mission.

12. Provide a mission requirements Verification Matrix that shows the pre launch verification of the mission level requirements. This matrix shall address both the fidelity and type of verification.

13. Identify all single point failures and provide a subjective assessment of the probability of each such failure mode causing a mission failure. Also provide adequate rationale to substantiate the subjective assessment.

The Red team shall critically review each of the above items and focus on implementation that could contain unevaluated risk to mission success.

5. Phased Review of Specific Topics

The 13 items above can be characterized as falling into two phases, namely planning and implementation results. For this reason, the Red Team will review certain of the items in what will be called the Phase 1 Review and the remaining items will be covered in the Phase 2 Review. The following is a listing by subparagraph number of those processes that will be covered in each review.

Phase 1 Review (Topics List)

1,2,3 (plans), 4, 5, 6, 9, 10 (plans), 11, 12 (plans), and 13

Phase 2 Review (Topics List)

3 (results), 7, 8, 10 (results), 12 (results)

6. Mission Unique Review of the Launch Vehicle

The KSC chartered Launch Vehicle Services Red Team will conduct a Mission Unique Review of the mission launch vehicle. The Mission Red Team Chairman will name the cross members from the Mission Red Team for this review.

7.In performing this task, the Red Team shall do the following:

1. Document the above review investigations in a summary matrix that indicates actual level of performance achieved on each of the above items. This should take into account the level of difficulty and complexity of each mission. Each of these items shall be rated on a scale of 1 to 10 with 10 being a very superior implementation and 7 being judged as nominal expected for assuring a remaining residual risk judged to be categorized as low. Each and every lapse in adequate implementation (a scoring of 6 or lower), even if the overall implementation is judged as being adequate, shall be identified and documented and judged under Item #2 below. Potential viable mitigation of remaining risk shall also be addressed if applicable.

2. Ascertain and document all residual risks, judged to be any level higher than low, that are remaining in the mission. Provide recommendations on methods and implementations to mitigate these identified higher-than-low risks.

3. Assess all single point failure mechanisms and provide a recommendation on the acceptability of non-acceptability, with appropriate rationale for each judgment.

4. Assess the FMEA, FTA and PRA for completeness. Where these analyses have not been performed or are not complete, the Team shall assess the work that has been done and shall assess the current situation in regards to available data for doing a FTA and a PRA that would include all non-core ELV elements of this mission. Specifically, in the Final Report**, <u>given the current state of the SORCE Mission implementation</u>,** provide definitive answers, to the following questions:
   - Can a meaningful FMEA, FTA and PRA be performed at this stage of the SORCE mission implementation, especially in regards to data and personnel availability?
   - If a FTA and/or a PRA were to be performed prior to the final decision to launch, what schedule impacts and costs of actual FTA and PRA performance would be associated with this work?
   - Would the performance of a PRA at this time add significantly to our knowledge of the risks of failure already derived from other assessments?
   - From a practical standpoint, can the probability of mission success be significantly enhanced by knowledge derived from the performance of a FMEA, FTA and a PRA at this time?

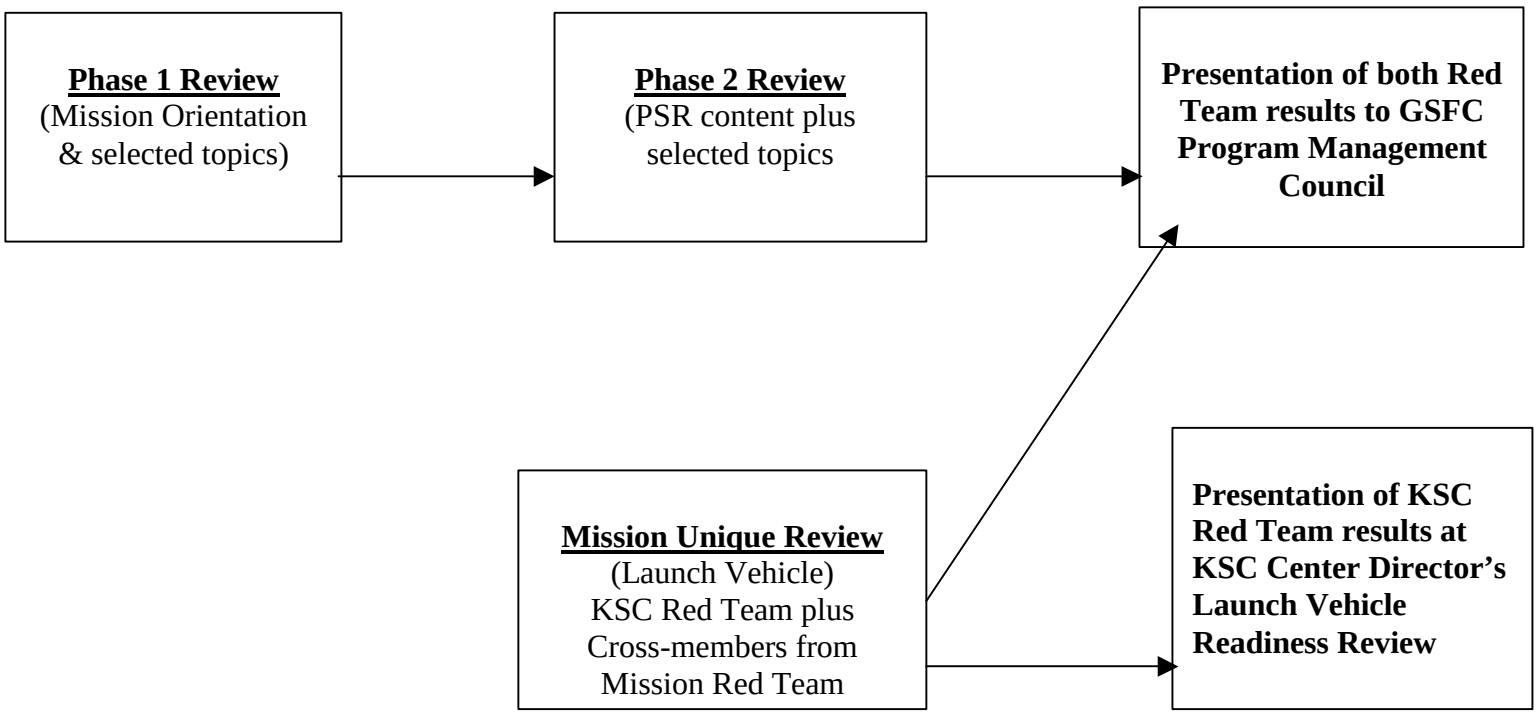
   If a PRA has not been done, the Red Team shall review (or develop) other available, relevant information and assign subjective levels of probability of occurrence and mission risk (criticality) to each identified mission failure mode. This shall be done using the International Space Station developed 5X5 matrix and definitions of low, medium, and high risk (See Attachment A)
5. Assess the level and thoroughness of the IV&V performed on mission critical software.
   Where IV&V has not been performed in compliance with draft NASA IV&V Policy and criteria (See Attachments B & C) assess the net value of performing IV&V at this stage in the program. Also identify any residual risks being taken in the Project because of the lack of IV&V.
6. Provide a report in the form of a presentation on all of the above to the Center Director and the Goddard Program Management Council in approximately two weeks of completing the final review of each mission (actual date to be scheduled). This shall include an overall mission risk statement, along with the justification for that statement.
7. Provide a written report within one week of the presentation to the Goddard PMC. This report can consist of the presentation charts used for the Goddard PMC presentation along with a cover letter and attachments that provide details of the specific review methodologies used by the Red Team along with any other pertinent information. This report shall be submitted to the Director of the Office of Systems Safety and Mission Assurance (Code 300) at the Goddard Space Flight Center.

Table 1
SORCE Red Team Reviews

#	Review Summary	Comments
1	**Phase One Review** Mission Orientation plus review of those topics listed under Phase 1 in Section 5	Could be combined in tandem with mission CDR provided it includes Orientation & Phase 1 specific topics in Section 5 of this charter
2	**Phase Two Review** (Essentially the same content as the mission Pre-Ship Review plus those topics listed under Phase 2 in Section 5)	Could be combined in tandem with mission PSR provided it includes Phase 2 specific topics in Section 5 of this charter
3	**Mission Unique Review** **(**Conducted by the KSC Launch Vehicle Services Red Team**)**	Selected members of the Mission Red Team will participate as cross-members in this review of the launch vehicle

SORCE
Red Team Review Summary
August 30, 2000

Figure 1



Attachment A
International Space Station Risk Matrix

Risk Matrix Scoring System from International Space Station Program

Approach to definition of Low, Medium and High Risks

Create a "5 X 5" matrix, with x axis "consequence", and y axis "probability of occurrence", as shown

P	5	x x x x x
R	4	x x x x x
O	3	x x x x x
B.	2	x x x x x
	1	x x x x x
		1 2 3 4 5

Consequences:

Source is the project criticality assessment (when provided).

5 Unacceptable technical, cost, or schedule impacts; loss of mission
4 Major impacts in technical, cost, or schedule; inability to meet mission requirements
3 Moderate impact with workarounds possible; can meet mission requirements, some loss of science
2 Moderate impact using same technical approach; minimal science impact
1 Minimal or no impact

Probability of Occurrence

Source is the judgment of the evaluator.

5 Very High
4 High
3 Moderate
2 Low
1 Very Low

Scoring:

Multiply the Criticality times the Probability of Occurrence to arrive at Risk Score

16 or higher	HIGH Risk
10 to 15	MEDIUM Risk
1 to 9	LOW Risk

Attachment B
NASA Policy Directive
Software Independent Verification and Validation
DRAFT
5/17/00

5/17/00

DRAFT

NASA POLICY DIRECTIVE

Directive: NPD 8XXX.X
Effective Date: XXX YY, 2000
Expiration Date: XXX YY, 2005

Responsible Office: Q/Office of Safety and Mission Assurance

Subject: Software Independent Verification and Validation

1. POLICY

It is NASA policy to --

a. Maximize the likelihood of mission success by using appropriate software independent verification and validation (IV&V) techniques, tools and processes to mitigate program and project risk.

b. Have all NASA programs, with Center SMA support and in consultation with the IV&V Facility staff, assess and document the need for IV&V.

c. Establish SMA focal points at each Center and Headquarters who will be responsible for coordinating with the NASA IV&V Facility for the identification, negotiation, documentation, and implementation of IV&V activities in support of programs and projects.

d. Establish the NASA IV&V Facility as the organization responsible for providing IV&V techniques, tools, processes, implementation and management in support of NASA programs and projects.

2. APPLICABILITY

This NPD is applicable to all PAPAC programs and projects being managed and implemented by NASA Headquarters and NASA Centers, including Component Facilities, and by the Jet Propulsion Laboratory. This NPD may also be selectively applied to non-PAPAC software efforts at the discretion of the Governing Program Management Council or the Capital Investment Council.

3. AUTHORITY

42 U.S.C. 2473(c)(1), Section 203(c)(1) of the National Aeronautics and Space Act of 1958, as amended.

4. REFERENCES

a. NPD 2820, NASA Software Policy
b. NPD 7120.4, Program/Project Management
c. NPD 8700.1, NASA Policy for Safety and Mission Success
d. NPG 7120.5, NASA Program and Project Management Processes and Requirements

5. RESPONSIBILITY

Each NASA organizational element has the responsibility for compliance with the policies set forth above, including the allocation and maintenance of appropriate levels of authority, funding, and training necessary for its fulfillment.

a. The Associate Administrator for Safety and Mission Assurance is responsible for the following:

(1) Providing executive leadership and policy direction on all Independent Verification and Validation (IV&V) issues for Enterprises, projects, programs, and mangers throughout NASA.

(2) Establishing leadership and implementation strategies to facilitate the deployment of IV&V across NASA Enterprises, programs and projects.

(3) Ensuring that effective and efficient SMA functional management is in place to facilitate appropriate application of IV&V to NASA programs, projects and operations.

(4) Providing oversight to ensure effective of IV&V resources and developing training and professional development initiatives to ensure that the NASA workforce is knowledgeable in IV&V concepts and techniques.

b. The NASA Chief Engineer is responsible for:

(1) Providing executive leadership for this policy implementation as a part of the Agency's Engineering Excellence Initiative.

(2) Supporting the development and rapid transfer of new IV&V technologies, tools, processes and techniques.

c. The Enterprise Associate Administrators are responsible for:

(1) Implementing Agency IV&V policy, plans and procedures on their programs and projects as appropriate.

d. The Governing Program Management Councils (GPMC) are responsible for the following:

(1) Making a determination on whether the selection of performance of IV&V is appropriate for a program or project under their cognizance.

(2) Reviewing the results of the IV&V process to assure that the software implementation meets the program, project and Agency needs.

e. The NASA IV&V Facility is responsible for:

(1) Managing all applicable IV&V efforts for the Agency.

(2) Coordinating with the programs and projects the implementation of the appropriate levels of IV&V products and services for specific programs and projects as determined by the GPMC.

(3) Developing and acquiring state-of-the-art IV&V tools and techniques.

(4) Providing support to the NASA Independent Program Assessment Office (IPAO), through providing access to latest IV&V information and/or representatives to serve on IPAO review teams.

(5) Supporting the development of IV&V training.

e. PAPAC program and project managers are responsible for the following:

(1) Implementing IV&V policies, plans, and procedures.

(2) Formulating, in conjunction with the Center SMA Functional Managers, the level of IV&V to be applied documenting the details in the program and project SMA plan.

6. DELEGATION OF AUTHORITY

None

7. MEASUREMENTS

None

8. CANCELLATION

None

/s/ Daniel S. Goldin
Administrator

ATTACHMENT A: (TEXT)

None

(URL for Graphic)

None

DISTRIBUTION:
NODIS

Attachment C
Proposed Appendix to NPG 2820
Independent
Verification and Validation (IV&V)
Criteria

Independent Verification and Validation (IV&V) Criteria

1. The purpose of this appendix is to establish quantifiable criteria for determining whether IV&V should be applied to a given software development. Since IV&V should begin in the Formulation Subprocess (as defined in NPG 7120.5, Section 1.4.3) of a project, the process here described is based on metrics which are available before project approval.

   These criteria shall be applied to NPG 7120.5 "projects" as defined in the NPG. Software developments outside the scope of NPG 7120.5 are determined to be within scope of this appendix on a case by case basis. That decision will be made by the NASA Chief Information Officer (CIO), the NASA Office of the Chief Engineer (OCE), and the NASA Office of Safety and Mission Assurance (Code Q) or Center Safety and Mission Assurance.

   Projects meeting the following criteria are not subject to this appendix, and need not be addressed further:

   a. The software product is only used for post mission scientific data analysis

   b. Consequences of software failure (Not to exceed any of the following)

      - Potential for loss of life - No
      - Potential for serious injury – No
      - Potential for catastrophic mission failure – No
      - Potential for partial mission failure – No
      - Potential for loss of equipment – Less than $2,000,000
      - Potential for waste of resource investment – Less than 20 work-years on software
      - Potential for adverse visibility – No more than local visibility
      - Potential effect on routine operations – No more than a Center inconvenience

2. IV&V is intended to assist mitigating risk; hence, the decision to do IV&V should be risk based. NPG 7120.5 defines risk as the "combination of 1) the probability (qualitative or quantitative) that a program or project will experience an undesired event such as cost overrun, schedule slippage, safety mishap, or failure to achieve a needed breakthrough; and 2) the consequences, impact, or severity of the undesired event were it to occur." The exact probability of occurrence and consequences of a given software failure cannot be calculated early in the software lifecycle.

However, there are realistically available metrics which give good general approximations of the consequences as well as the likelihood of failures.

2.1 In general, the consequences of a software failure can be derived from the purpose of the software: i.e., what does the software control; what do we depend on it to do. Section 2.1.1 contains a list of factors, which can be used to categorize software based on its intended function as well as the level of effort expended to produce the software. Section 2.1.2 defines the boundaries of four levels of failure consequences based on the rating factors from 2.1.1.

2.1.1 Factors contributing to the consequences of software failure:

2.1.1.1 Potential for loss of life. Is the software the primary means of controlling or monitoring systems that have the potential to cause the death of an operator, crewmember, support personnel, or bystander? The presence of manual overrides and failsafe devices are not to be considered. This is considered a binary rating: responses must be either yes or no. Examples of software with the potential for loss of life include:

- Flight and launch control software for manned missions
- Software controlling life support functions
- Software controlling hazardous materials with the potential for exposure to humans in a lethal dose
- Software controlling mechanical equipment (including vehicles) which could cause death through impact, crushing, or cutting
- Any software which provides information to operators where an inaccuracy or misinterpretation of the data could result in death through an incorrect decision (e.g., mission control room displays)

2.1.1.2 Potential for serious injury. Serious injury is here defined as loss of digit, limb, or sight in one or both eyes, sudden loss of hearing, or exposure to substance or radiation that could result in long term illness. This rating is also binary. This rating considers only those cases where the software is the primary mechanism for controlling or monitoring the system. The presence of manual overrides and failsafe devices are not to be considered. Examples of software with potential for serious injury include software controlling milling or cutting equipment, class IV lasers, or X-ray equipment.

2.1.1.3 Potential for catastrophic mission failure. Can a problem in the software result in a catastrophic failure of the mission? This is a binary rating. Software controlling navigation, communications, or other critical systems whose failure would result in loss of vehicle or total inability to meet mission objectives would fall into this category.

2.1.1.4 Potential for partial mission failure. Can a problem in the software result in a failure to meet some of the overall mission objectives? This is a binary rating. Examples of this category include software controlling one of several data collection systems or software supporting a given experiment, which is not the primary purpose of the mission.

2.1.1.5 Potential for loss of equipment. This is a measure of the cost (in dollars) of physical resources that are placed at risk due to a software failure. Potential collateral damage is to be included. This is exclusive of mission failure. Examples include:

- Loss of a $5 million unmanned drone due to flight control software failure. (Assuming the drone is replaceable, this wouldn t be a mission failure)
- Damage to a wind tunnel drive shaft due to a sudden change in rotation speed.

2.1.1.6 Potential for waste of software resource investment. This is a measure or projection of the effort (in work-years, civil service, contractor, etc.) invested in the software. This shows the level of effort that could potentially be wasted if the software doesn t meet requirements.

2.1.1.7 Potential for adverse visibility. This is a measure of the potential for negative political and public image impacts stemming from a failure of the system as a result of software failure. The unit of measure is the geographical or political level at which the failure will be common knowledge—specifically: local (Center), Agency, national, international. The potential for adverse visibility is evaluated based on the history of similar efforts.

2.1.1.8 Potential effect on routine operations. This is a measure of the potential to interrupt business. There are two major components of this rating factor: scope and impact. Scope refers to who is affected. The choices are Center and Agency. The choices for impact are inconvenience and work stoppage. Examples:

- A faulty firewall which failed to protect against a virus resulting in a 4-hour loss of e-mail capabilities at Goddard would be a "Center inconvenience".

- Assuming that the old financial management software was no longer maintainable, the failure of the replacement system to pass acceptance testing and the resulting 2-year delay would be a potential "Agency work stoppage." This doesn t imply that

workarounds couldn t be implemented, but only that it has the potential to stop work Agencywide.

2.1.2 Software Consequences of Failure Rating

2.1.2.1 Consequences of failure are considered "Grave" when *any* of the following conditions are met:

- Potential for loss of life - Yes
- Potential for loss of equipment – Greater than $100,000,000
- Potential for waste of resource investment – Greater than 200 work-years on software
- Potential for adverse visibility - International

2.1.2.2 Consequences of failure are considered "Substantial" when *any* of the following conditions are met:

-
- Potential for serious injury – Yes
- Potential for catastrophic mission failure – Yes
- Potential for loss of equipment – Greater than $20,000,000
- Potential for waste of resource investment – Greater than 100 work-years on software
- Potential for adverse visibility - National
- Potential effect on routine operations – Agency work stoppage

2.1.2.3 Consequences of failure are considered "Marginal" when *any* of the following conditions are met:

- Potential for partial mission failure - Yes
- Potential for loss of equipment – Greater than $2,000,000
- Potential for waste of resource investment – Greater than 20 work-years on software
- Potential for adverse visibility - Agency
- Potential effect on routine operations – Center work stoppage or Agency inconvenience

2.1.2.4 Consequences of failure are considered "Insignificant" when *all* of the following conditions are met:

- Potential for loss of life - No
- Potential for serious injury – No
- Potential for catastrophic mission failure – No
- Potential for partial mission failure – No
- Potential for loss of equipment – Less than $2,000,000

- Potential for waste of resource investment – Less than 20 work-years on software
- Potential for adverse visibility – No more than local visibility
- Potential effect on routine operations – No more than a Center inconvenience

2.2 The probability of failure for software is difficult to determine even late in the development cycle. However, Table 1 contains simple metrics on the software, the developer, and the development environment, which have proven to be indicators of future software problems. While these indicators are not precise, they provide order of magnitude estimates, which are adequate for assessing the need for IV&V. (The IV&V Facility and the NASA Software Working Group will further refine these indicators and their associated weighting factors as more data becomes available.)

3. Combining the software consequences of failure and the likelihood of failure rating from Section 2 yields a risk assessment, which can be used to identify the need for IV&V. The indication of whether IV&V is required is obtained by plotting in Figure 1 the intersection of the Consequences of Software Failure determination and the Total Likelihood of Failure determination. Application of these criteria simply determines that a project is a candidate for IV&V – not the level of IV&V nor the resources associated with the IV&V effort. These will be determined as a result of discussions between the project and the IV&V Facility.

3.1 Figure 1 shows a dark region of high risk where software consequences, likelihood of failure, or both are high. Projects having software that falls into this high-risk area shall undergo IV&V. The exception is those projects which have already done hardware/software integration. An IV&V would not be productive that late in the development cycle. These projects shall undergo a Software Independent Assessment (IA). (See Section 3.2.)

3.2 Figure 1 shows three gray regions of intermediate risk. Projects having software that falls into these areas shall undergo a Software IA. The IV&V Facility shall conduct the Software IA according to established IV&V Facility procedures. One purpose of the Software IA is to ensure that the software development does not have project-specific risk characteristics that would warrant the performance of IV&V. Should such characteristics be identified, a recommendation for IV&V performance will be made.

4. All projects containing software shall evaluate themselves against the criteria of this document to determine if a Software IA or an IV&V is

required and shall notify their Governing Program Management Council (GPMC) and/or the Center Director of the results. Projects identified as candidates for IV&V or Software IA shall be contacted by the IV&V Facility to discuss the appropriate level of effort to be applied.

Factors contributing to probability of software failure	**Un-weighted probability of failure score**					**Weighting Factor**	**Likely-hood of failure rating**
	1	2	4	8	16		
Software team complexity	Up to 5 people at one location	Up to 10 people at one location	Up to 20 people at one location or 10 people with external support	Up to 50 people at one location or 20 people with external support	More than 50 people at one location or 20 people with external support	X2	
Contractor Support	None	Contractor with minor tasks		Contractor with major tasks	Contractor with major tasks critical to project success	X2	
Organization Complexity*	One location	Two locations but same reporting chain	Multiple locations but same reporting chain	Multiple providers with prime sub relationship	Multiple providers with associate relationship	X1	
Schedule Pressure**	No deadline		Deadline is negotiable		Non-negotiable deadline	X2	
Process Maturity of Software Provider	Independent assessment of Capability Maturity Model (CMM) Level 4, 5	Independent assessment of CMM Level 3	Independent assessment of CMM Level 2	CMM Level 1 with record of repeated mission success	CMM Level 1 or equivalent	X2	
Degree of Innovation	Proven and accepted		Proven but new to the development organization		Cutting edge	X1	
Level of Integration	Simple - Stand alone				Extensive Integration Required	X2	
Requirement Maturity	Well defined objectives - No unknowns	Well defined objectives - Few unknowns		Preliminary objectives	Changing, ambiguous, or untestable objectives	X2	
Software Lines of Code***	Less than 50K		Over 500K		Over 1000K	X2	
Total							

Table 1 Likelihood of Failures Based on Software Environment

The following notes and definitions apply to Table 1:

*** Organization complexity is an indirect measure of communications challenges inherit in the software developer. A single organization working from multiple locations faces a slightly greater challenge than an organization in one location. When the software development is accomplished by multiple organizations working for a single integrator, the development is significantly complicated. If the developing organizations are coequal such as in an associate contractor relationship (or a similar relationship between government entities) then there is no integrator. Experience has shown this arrangement to be extremely challenging as, no one is in charge.**

**** Under "schedule pressure" a deadline is negotiable if changing the deadline is possible although it may result in slightly increased cost, schedule delays, or negative publicity. A deadline is non-negotiable if it is driven by immovable event such as an upcoming launch window.**

*** As the problems identified in IV&V are often mismatches between the intended use and the actual software built, "software lines of code" shall include reused software and autogenerated software.

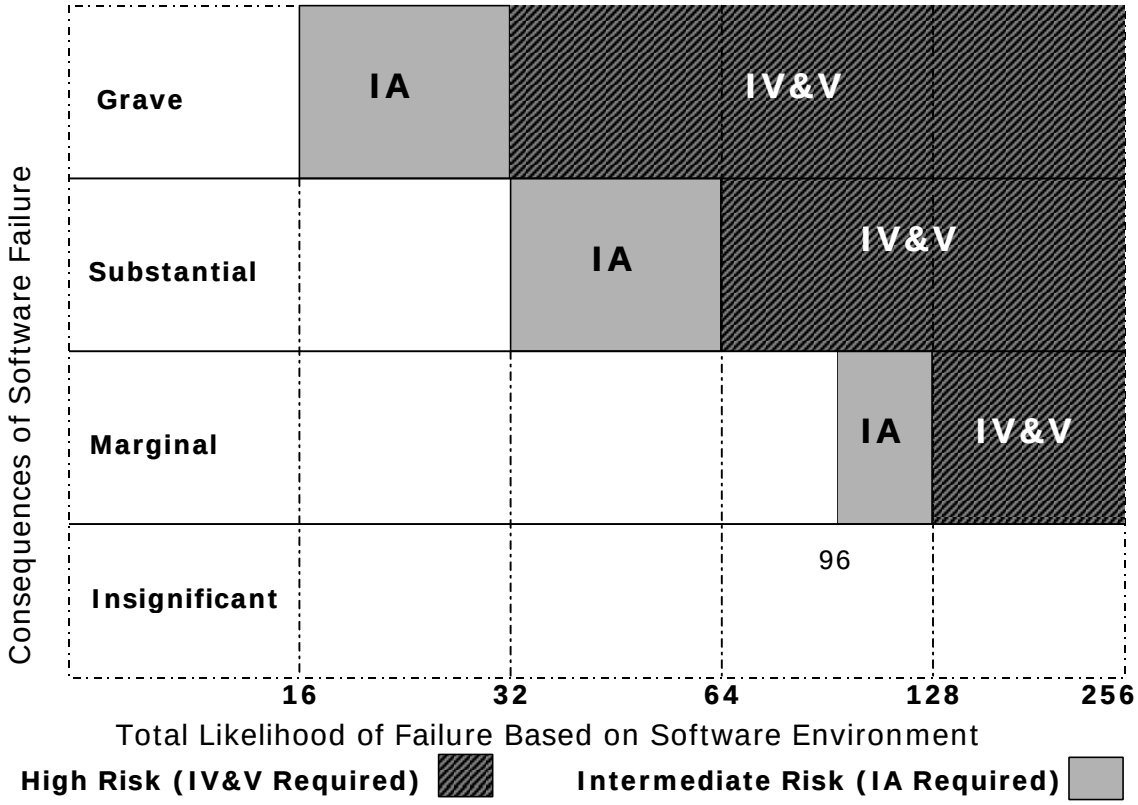


Figure 1 Software Risk